数据交易平台经营者安全保障义务的规范构造*

李倩[1] 李海美[1]

昆明理工大学法学院，昆明 650500

摘要：［目的/意义］为促进数智时代交易场所强化合规管理，打造安全可信流通环境，围绕数据交易平台经营者的安全保障义务进行制度设计尤为重要。**［方法/过程］**数据交易平台作为新型经营场所，其经营者的安全保障义务的正当性可由获利报偿理论、控制力理论与信赖保护等理论得以证成。**［结果/结论］**从传统经营场所、电子商务平台到数据交易平台，由于经营者的风险控制力等因素差异，三者呈现出安全保障义务与民事责任水平递增的类型序列。数据交易平台经营者的安全保障义务的内容应包括资质资格审核、提供安全可靠的交易环境、记录交易痕迹等交易前、中、后义务。在有其他侵权人介入时，对数据交易平台责任形态的认定应通过部分连带责任进行规范续造，以合理确定数据交易平台经营者的民事责任。

关键词：数据交易平台；安全保障义务；经营场所；侵权责任

Normative Construction of Security Obligations for Operators of Data Trading Platforms

Li Qian Li Haimei

Kunming University of Science and Technology, Law School, Kunming 650500

Abstract: ［**Purpose/Significance**］In order to promote the compliance management of trading places in the era of digital intelligence and create a safe and credible circulation environment, it is particularly important to design the system around the security obligations of operators of data trading platforms. ［**Method/Process**］As a new business place, the data trading platform's operators' security obligations can be justified by the theories of profit reward, control power and trust protection. ［**Result/Conclusion**］From traditional business premises, e-

*本文系 2021 年教育部新文科研究与改革实践项目“智慧环境下法学五维教学方式的改革研究”（2021180029）研究成果之一；2022 年度昆明理工大学人文社科培育项目“我国数据出境标准合同的规制完善研究”（PYYB2022005）研究成果之一。

[1] **作者简介**：李倩，副教授，博士，硕士生导师，通讯作者，E-mail：2159486621@qq.com；李海美，硕士研究生。

commerce platform to data trading platform, due to the differences in risk control power of operators and other factors, the three show a type sequence of increasing security obligations and civil liability levels. The security obligations of data trading platform operators should include pre-, mid-and post-transaction obligations such as qualification examination, providing a safe and reliable trading environment and recording trading traces. When other infringers are involved, the determination of the liability form of the data trading platform should be standardized and continued through part of joint liability, so as to reasonably determine the civil liability of the operators of the data trading platform.
Keywords: Data Trading Platform Security Obligations Business Premises Tort Liability

1 引言

2023 年 12 月，国家数据局等部门印发《“数据要素×”三年行动计划（2024—2026 年）》，再次强调“鼓励交易场所强化合规管理”“打造安全可信流通环境”。这是继 2022 年底《国务院关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）正式提出“建立数据可信流通体系”的总体目标以及“统筹构建规范高效的数据交易场所”“鼓励各类数据商进场交易”之后，对数据交易平台合规化、可信化提出的进一步具体构想。在我国，大数据交易平台以数据交易所为主要模式，其业务为向数据要素市场提供以交易撮合为基础的一揽子服务。尽管大数据交易平台并非唯一交易渠道，但由于其在建立交易互信、促进数据合规等方面的应然优势，我国自 2014 年以来相继设立数十个数据交易平台，并持续释放利好政策，数据交易已进入 2.0 时代。然而，近十年间数据交易平台举步维艰，现有数据交易平台中数据产品和服务的种类尚不够丰富，场内交易的规模和活跃度远低预期。其中，数据交易平台的安全保障义务模糊不清是其合规建设与吸引交易的重要障碍之一。

我国民法中关于安全保障义务的规定主要见于《民法典》第 1198 条、《电子商务法》第 38 条等条文，但由于其条文之间体系解释方法的固有争议，以及该安全保障义务能否直接适用于数据交易平台有待探讨，因此数据交易平台的安全保障义务相关规则尚不清晰。在法学界现有对安全保障义务的研究中，从

义务主体视角看，主要包括医疗机构、体育运动场域、电子商务平台、网络视频平台、网上银行、数字人民币运营机构等，尚未涉及对数据交易平台这一新兴主体的特别关注。由于我国场内数据交易的实践样本不够丰富，学界对数据交易平台的法律规范研究也较为宏观，对微观层面的义务探讨较少。鉴于此，本文将在分析当下数据交易平台经营者角色定位的基础上，探讨其承担安全保障义务的理论基础与具体内容，并澄清数据交易平台经营者违反安全保障义务的侵权责任，为场内数据交易的可信化提供私法基础。

2 数据交易平台经营者安全保障义务的立法不足

从数据交易平台的实践现状看，场内数据交易的安全性直接影响着交易的活跃度。当前，绝大部分数据交易活动在场外进行，[1]2022 年场内交易约占整体市场的 5%。[2]国家工业信息安全发展研究中心发布的《2022 年数据交易平台发展白皮书》明确指出，“交易风险较高，影响了交易行为的发生”。[3]其中，由于数据来源用途不透明、云存储安全漏洞等因素的存在，场内数据交易仍存在数据泄露风险、隐私侵害风险、数据滥用风险等。只有数据交易平台有效控制此类风险的发生，才能真正吸引数据交易商进场交易。

我国现有法律法规对数据交易平台安全保障义务的供给较为薄弱，这是场内交易存在“信任困境”的重要原因之一。[4]其中较为直接的法律依据主要为我国《数据安全法》第 33 条，该条明确规定了“从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录”，但该条范围较窄，难以囊括数据交易平台的主要安全保障义务内容。我国理论界中经典的一般安全保障义务的规范依据为《民法典》第 1198 条，而不包括第 1195 条等条文规定的网络服务提供者民事责任的避风港规则与红旗规则，而数据交易平台是否属于该条规定的“经营场所、公共场所的经营者、管理者”仍有待商榷。与之同理，《电子商务法》第 38 条第 2 款也对电子商务平台的安全保障义务进行了规定，但数据交易平台是否能够直接适用电子商务平台的法律规范也尚不明确，且该条款本身在理论与实践中的争议也较大。因此，数据交易平台的安全保障义务的法律架构有待设立。

3 数据交易平台经营者特殊安全保障义务的正当性

3.1 数据交易平台经营者安全保障义务的理论渊源

数据交易平台的安全保障义务具有深厚理论基础。一般性安全保障义务的来源在学理上包括获利报偿理论、控制力理论、信赖保护理论、企业责任理论、风险开启理论、法定义务理论、节约社会总成本理论等。其中，前三类理论对于数据交易平台安全保障义务的正当性证成较为重要，具体分析如下：

第一，获利报偿理论。大数据交易平台的交易和运营都以盈利为目的，具有明显的盈利性特征。一方面，数据交易双方通过大数据交易平台交易，享受平台提供的服务是以双方向平台支付对价为前提的。另一方面，即便平台未直接收取费用，平台仍然根据多边市场结构特征获取收益。具体而言在多边市场结构中，存在两个以上通过平台相互影响的群体，其中一个群体加入平台的获益取决于同一平台的另一个群体的数量。在多边市场环境中，平台通过免费或低价吸引大量数据需求方入驻，进而提高平台吸引力，促使更多的数据供给方愿意付出成本加入平台以接触到更大的潜在市场。这种情况下，尽管数据需求方可能不直接付费，但数据供给方为了获得更广泛的分发渠道和潜在客户，会向平台支付各种形式的费用，如会员费、展示费或成功撮合交易后的分成。因此，大数据交易平台在数据交易中获取利益的同时，也需承担不利的风险，承担安全保障义务。

第二，控制力理论。于受害人而言，基于数据的无形性、易复制性、传播快等特征和数据交易涉及多个数据处理环节，取证时技术要求高，证据易篡改等因素，受害人维权成本过高，使得受害人陷入维权难的境地。反之，大数据交易平台作为数据交易的主导者更了解数据交易的流程以及各流程下的服务，同时平台具有极强的数据控制优势，基于此大数据交易平台具备更强的风险预见力。同时根据社会最低成本考虑，大数据交易平台通过技术和管理手段，可以从源头上进行管控，以及在很大程度上减少数据交易过程中的各类风险，通过自动化和规范化操作，节省人力成本，实现最低成本的风险防控。因此，在大数据交易环境下，由大数据交易平台承担安全保障义务是从经济效率和可持续发展的角度出发的合理选择。

第三，信赖保护理论。信赖利益是市场参与者之间建立合作关系的基础，只有确保交易各方基于对平台的信任进行数据交易，市场才能形成稳定的合作秩序和良性循环。与场外交易相比，解决数据供需双方因信息不对称引发的信任危机以及保障数据安全是大数据交易平台的显著优势，也是平台运营的必要要求。数据供需双方基于大数据交易平台公开的信息和承诺，以及平台的交易规则等产生合理的信赖，包括相信平台本身是安全可靠的，以及不论是在技术上还是管理上平台都有防范风险的能力和具体的应对措施，最后在对平台产生合理信赖的基础上通过平台进行交易。因此基于数据供需双方在交易时对平台的合理信赖，平台有必要承担安全保障义务。

总体来看，对于线上数据交易可能带来数据泄露、隐私侵权等风险，平台具有较强的控制力与责任承担能力。因此，由盈利性数据交易平台控制主要交易风险并承担相应不利后果，是社会总成本最小、规范效果最佳的方案，也是场内数据交易可信化建设的重要抓手。

3.2 数据交易平台经营者安全保障义务的特殊性

数据交易平台可被定位为“新型经营场所”，从而可以适用《民法典》第1198条第1款关于安全保障义务特殊责任主体的基本规定。从各地数据交易平台的实践来看，数据交易平台运营模式有所不同，一类是纯第三方交易模式，即数据撮合交易模式，平台主要为数据供需双方的数据交易提供桥梁作用；另一类是数据增值服务模式，即综合数据服务模式，除基础的交易撮合业务外，还为数据供给方提供的数据进行清洗、建模、分析、可视化处理等综合数据服务。同时，尽管数据交易平台存在线下运营的环节，但由于数据这一交易对象的电子化特征，线上操作是平台运营的主要场景。从这一角度看，虽然数据交易平台存在不同的运营模式，该正如电子商务平台中兼容中介模式与自营模式，该运营模式的不同不影响其成为安全保障义务主体，且网络平台的非物质性并不阻碍其承担安全保障义务的合理性。[5]因此，数据交易平台可初步被作为经营场所的经营者与电子商务平台经营者，它们在承担安全保障义务的内容上具有一定的相似性。

然而，从义务与责任的程度来看，数据交易平台应该比普通的经营场所、电子商务平台有着更为严格的规范机制。这一差异集中体现在平台内经营者直

接侵权、且平台违反安全保障义务间接侵权的多数人侵权场景。从多数人侵权中“多数人”之间的关系看，三个主体具有实质性差异，从“经营场所”“电子商务平台”到“数据交易平台”呈现出责任主体之间关系逐渐密切，对案涉场所的控制力逐渐增强，从而安全保障义务与责任更重的类型序列。正如有学者所言，平台的数据安全保障义务的扩张,实际上是数字经济社会生产中膨胀的平台权力的纠偏机制。[6]多数人侵权中的第三人可能是场所内的经营者，或是场所外的不特定主体。在传统的商场等经营场所中，进入场所的主体数量极其有限且往往无法实名制，侵权人的行为轨迹难以全部记录，且场所经营者对安全风险的控制主要靠人力；在电子商务平台之中，数字化技术使得进入平台的主体海量化，主体的实名制能够实现，主体的行为有迹可循且平台对侵权风险的控制力显著增强。有学者将后者总结为“经营者集合商、商品交易运营者、交易秩序管理者、纠纷调解裁决者”“具有社会公共性”。[7]而对于新兴的数据交易平台而言，除了具备电子商务平台的基本特征外，加之数据的无形性、易复制性、传播快，以及数据产品的质量、价值难以直观评估等特殊原因，尽管立法对其安全保障义务仅有零星规定，但在数据交易可信化的场内交易建设目标之下，为鼓励数据商进场交易，数据交易平台应具备更高水平的安全保障义务与相应责任。

4 数据交易平台经营者安全保障义务的具体化

我国场内数据交易还处于起步阶段，现有法规、政策尚未像证券交易所、电子商务平台那样出台较为细致的安全保障义务规定。学理上一般认为安全保障义务的具体内容与限度要综合考虑致害风险的大小、可能损害的严重程度、防范风险实现的成本等因素予以认定。[8]基于此，数据交易平台的安全保障义务应分为数据申请、数据审核、发布需求、数据交易、数据应用这五个运营步骤分为交易前、中、后三阶段，做到事前审查、事中保障、事后监督与救济。

4.1 交易前义务

交易前包括数据申请、数据审核、发布需求三个步骤。具体为数据供给方向平台提交数据交易申请，平台对其数据进行审核和上线，数据需求方发布数

据需求。该阶段主要面临数据隐私风险和质量风险，对此平台负有对入场交易者的资质资格审核义务、数据审核义务以及告知说明义务，严格实行事前审查。

首先，负有资质资格审核义务。在开展数据交易活动之初，平台运营商肩负着极为关键的职责，即执行严谨的数据供给方资质与资格审核程序。为了维护交易平台的秩序与信誉，针对数据供应机构，普遍实施一种基于会员制度的进入门槛机制。这一机制的核心在于深入核实潜在参与者的企业合法性及其商业信用背景，这是构建安全可靠的大数据交易环境的基础环节。值得注意的是，在现行法规尚未形成对所有交易主体统一资格标准的情况下，不同大数据交易平台在实际运作中采用了多样化的准入流程。以贵阳大数据交易所为例，它推行了一种典型的会员制准入模式，强调对申请加入的交易主体实行深度核查，不仅对其法人身份、业务范围等合法性进行全面确认，还特别关注其历史信用记录及持续经营能力，以此作为接纳新会员的标准。与此同时，另一种如哈尔滨数据交易中心所践行的登记制准入方式也应运而生。这种制度相对较为宽松，倾向于快速便捷的线上认证过程，往往不要求过于严苛的前置条件审查。登记制下的交易主体获取数据交易资格的过程可能仅需满足基本的线上信息登记和必要的身份验证，而不必经历复杂的资质审核程序。两种不同的准入制度反映出大数据交易市场在探索有效监管与灵活开放之间的平衡，同时也体现出各地政策实践因地制宜的特点。

其次，负有数据审核义务。通过形式审查，审核数据的合法性以及合目的性。具体而言，平台首先负有数据来源的隐私安全保障义务，具体审核数据供给方提供的数据来源是否合法，数据内容是否已脱敏，是否具有使用权限，如使用个人数据要满足“告知——同意”程序等；第二，平台应审核数据需求方数据用途是否合法，事前预防数据非法交易，防范数据使用安全问题。第三，平台负有对数据产品或服务的质量控制义务，了解数据供方和需方的基本数据类型，实现供需对接，为数据需求方提供高质量的数据。

最后，负有告知说明义务。数据交易以网络技术为依托，网络空间的虚拟性、非面对面性决定了用户方在选择某一项数据服务时很大程度上依赖于平台方对该服务事项所发布的事前信息说明。[9]在买卖合同履行之前，交易双方对数据产品的内容往往并无清晰的了解，且一经履行，数据产品的退货机制可能

难以运行。针对数据交易的“质量检验”[10]难题，数据交易平台作为中立的第三方，应在合理限度内将数据产品的类型、价值与可能风险提前告知买方，在保障数据安全与商业机密的前提下促进双方互信。

4.2 交易中义务

在交易中阶段的数据交易细分为交易确认和结算。平台根据数据需求方的数据需求类型与符合条件的数据供给方对接，由数据需求方通过平台向数据供给方提出申请，数据供给方通过平台进行交易确认，即双方合同成立，数据供给方提供特定的数据，数据需求方支付价款。作为数据交易的媒介，提供稳定、高效的交易技术是平台运行的前提，具备安全可靠的交易环境则为平台运行的保障。一方面，平台要满足安全稳定的技术条件，保证交易双方意思表示和数据的准确传输。另一方面，要建立完善的风险预警机制，即定期开展风险评估，及时进行数据风险监测和漏洞补救，发生数据安全问题及时应对和报告，对该类风险的应对可参照《数据安全法》第 29 条、第 30 条对于数据处理者的相关要求。因平台技术问题导致交易双方意思传达错误、数据传输不能甚至发生数据泄露风险的，平台应承担相应责任。

4.3 交易后义务

数据的后续使用中存在数据供需双方不合法使用数据的风险。一方面，数据需求方不在约定范围内使用数据，私自处分，损害数据供给方的财产权益，对数据进行再识别，损害数据主体的隐私权；另一方面，数据供给方违反合同约定，再次售卖数据等也会损害数据需求方的财产权益。作为数据交易的最后阶段，平台具有监督和自力救济的义务，主要包括负有对交易痕迹的妥善记录义务、数据追踪义务等。

具体来看，平台应在交易后负有对交易痕迹的妥善记录义务。数据交易从缔约到履行及运行均依赖网络技术，产生纠纷时便会出现举证难、维权难的尴尬境地。平台作为交易环境提供方，应对交易产生的信息进行记录和保存，当数据供需一方非法侵害另一方的权益时，便于向另一方提供证据，节约维权成本。对于保存的时间，可参考有关交易平台保存交易记录的规范，交易记录、交易者身份信息记录备份的时间应从交易完成之日起不少于两年。[11]同时，数据交易平台负有事后的数据追踪义务。数据交易平台需监督数据双方的数据使

用，超出合同约定的使用范围或私自转售的，及时通知数据交易的另一方。同时，在明确数据风险类型的基础上，设置分级监督机制，其中根据数据风险等级不同，监督力度亦不相同。

5 数据交易平台经营者违反安全保障义务的侵权责任

在数据交易平台经营者违反安全保障义务引发侵权责任时，根据直接侵权人的不同，可以分为安全保障义务人的侵害与第三人侵害这两种类型。在进行具体归责时，应在对《民法典》第 1198 条中传统安全保障义务与《电子商务法》第 38 条第 2 款特殊安全保障义务条款进行合理体系解释的基础上，澄清数据交易平台这一特殊责任主体承担侵权责任的法律适用方法。

5.1 无第三人介入的侵权责任

当数据交易平台违反了防止交易主体遭受平台自身侵害的安全保障义务，该损害后果的产生与第三人无关，诸如平台技术失灵导致数据泄露，则平台经营者是独立的责任主体，承担一般的过错侵权责任。在具体的法律依据上，由于责任主体单一，其不涉及对直接适用《民法典》第 1198 条第 2 款或《电子商务法》第 38 条第 2 款等理论争议，对其构成要件的检视可直接适用《民法典》第 1165 条。学界根据对该条文的不同解释，形成了侵权责任构成上的“三要件说”与“四要件说”，其不同之处在于是否采“违法性”要件。但是在违反安全保障义务的侵权责任构成上，通常都认为，违法性要件隐含在违反安全保障义务的过错判定或者损害认定之中，不需要再单独考虑违法性要件。[12]因此，本文也主要采“三要件”说。其中，对过错的认定较为简单，若数据交易平台经营者在三个阶段未能履行对交易主体的安全保障义务，一般可据此推定其在主观上存在过错。下文将探讨在无第三人介入的情形下，数据交易平台违反安全保障义务引发侵权责任的损害与因果关系构成要件的具体认定。

侵权法的首要功能即在于填补损害,若无损害,自无填补之必要。[13]损害通常分为财产损害和非财产损害。数据交易平台中参与交易的合同当事人一般是商事主体，即数据收集者、处理者等，一般并非作为自然人的数据来源。因此，数据交易平台违反安全保障义务对权利人造成的损害大多为财产损害，也包括

精神损害。对财产损害而言，依目前主流的差额说理论，该损害主要根据侵权行为前后的差额计算，包括实质财产的减少以及财产应增加而未增加。不过，在因平台技术问题导致未经清洗的敏感个人信息泄露等情形下，数据交易平台经营者也可能直接构成对作为个人信息来源的自然人的侵权，这种损害主要是非财产损害。

根据主流的相当因果关系说，在数据交易平台经营者违反安全保障义务的侵权责任的因果认定中，应进行条件性与相当性两个阶段的判断。申言之，假设平台经营者履行了对交易参与者的安全保障义务，相关的数据权益不一定会遭受侵害，则能够认定符合数据交易平台经营者的行为和相关数据权益受侵害之间因果关系的条件性。在对该相关性的具体解释中，为避免对数据交易主体苛加过重的证明负担，无须证明到“若数据交易平台履行了安全保障义务，那么数据权益必然不受侵害”的程度。在对相当性的判断中，需要证明数据交易平台所应采取的安全保障措施实质上会降低数据权益遭受侵害的概率。

5.2 有第三人介入的侵权责任

在有第三人介入的情形下，数据交易平台经营者违反安全保障义务引发的侵权责任一般为多数人侵权，其责任认定的难点在于具体的责任形态。在具体的法律依据上，其关键在于能否直接适用《民法典》第 1198 条第 2 款或《电子商务法》第 38 条第 2 款。对于这两个条文的体系关联，学界主要有两种观点，即“一般与特殊”或“原则与例外”的关系。[14]具体的观点分歧源于，在安全保障义务的视域下，应否认定“经营场所、公共场所的经营者、管理者”与“电子商务平台经营者”的一致性。更确切地说，若其本质一致，则对后一特殊条文的解释可以回归于作为一般规范的《民法典》第 1198 条，即造成损害的第三人承担侵权责任，数据交易平台经营者承担补充责任；若其本质不同，则对《电子商务法》第 38 条第 2 款解释可以背离或超越《民法典》第 1198 条，学界对具体的解释路径也有诸多方案。但对于数据交易平台而言，前述两个法条作为其安全保障义务规范依据均有不妥之处。前已述及，从传统经营场所、电子商务平台到数据交易平台，由于经营者的风险控制力等因素差异，三者呈现出安全保障义务与民事责任水平递增的类型序列。因此，对于《民法典》第 1198 条第 2 款中规定的场所经营者的补充责任，学界普遍认为即使是普通的电

子商务平台，也不应适用该责任形态，[15]更遑论风险风控制力更强的数据交易平台。此外，《电子商务法》第 38 条第 2 款规制的对象仅为“关系消费者生命健康的商品或者服务”，其对一般性的安全保障义务及责任未进行明确规定，且该法条中“相应的责任”在解释上众说纷纭，加之前述数据交易平台与电子商务平台的微妙区别，《电子商务法》第 38 条第 2 款也难以直接作为数据交易平台在该情形下的归责依据。

对于数据交易平台这一新兴主体，其侵权形态应适用特殊规则。数据交易平台经营者违反安全保障义务造成的多数人侵权中，其责任形态的认定应进行法律续造。申言之，当其他侵权人直接实施了加害行为，且平台经营者违反安全保障义务，两者共同造成损害的，需根据其他侵权人的主观状态进行责任划分。

若其他侵权人为故意侵权，平台应承担部分连带责任。从适用条件分析，侵权人积极实施侵权行为时，以平台不作为义务行为发生之日起即可认为平台行为与积极侵权人的行为在原因力上存在叠加关系，行为主体兼有故意和过失，符合部分连带责任的适用条件。若其他侵权人为过失侵权，两者应承担按份责任。双方主观可归责性一样，在法律责任上应作相同评价，按客观过错程度进行相应处罚。该方案与《民法典》第 1198 条第 2 款的补充责任相比，较为公允地针对平台未履行义务赋以明确不利后果，以倒逼其切实承担安全保障义务，同时很大降低了受害人的举证难度和救济成本，由平台承担部分连带责任是有效平衡三方权利义务关系的较好选择。

6 结束语

在数据要素价值化的进程中，为吸引数据商进场交易，数据交易平台的合规建设是关键抓手。尽管对数据交易平台的刑事合规、政府监管都至关重要，但针对其安全保障义务及义务违反的民事侵权责任规范是最为基础的一环，也是在数据商群体中建立信任的重要举措。作为数智时代的全新交易类型，场内数据交易的模式、体系、流程等都尚未成熟，本文对于数据交易平台经营者在事前、事中与事后的安全保障义务设计主要是基于当前有限的法律基础与实践需求。在对数据交易平台经营者违反安全保障义务的侵权责任厘定中，将其分

为两类予以分析：在无第三人介入时，按照一般侵权责任进行构成要件的解释；在有第三人介入时，通过多数人侵权中的部分连带责任进行规范续造，以期合理确定数据交易平台经营者的民事责任，提供数据流通与数据安全的平衡之策。

参考文献/References：

[1] 陈宏民,熊红林,胥莉等.基于平台视角下的数据交易模式及特点分析[J].大数据,2023,9(02):56-66.

[2] 张琦.以国家数据交易所为核心 加快构建多层次数据要素市场[N].上海证券报,2024-03-03(02).

[3] 殷利梅. 2022 年数据交易平台发展白皮书[R].2022.

[4] 麦买提・乌斯曼.个人数据交易平台交易后怠于履行数据安全管理义务行为的刑法规制[J].青少年犯罪问题,2024(01):62-81.

[5]米新丽,刘正之.论电子商务平台的安全保障义务[J].行政管理改革,2020(11):48-54.

[6]张凌寒.数据生产论下的平台数据安全保障义务[J].法学论坛,2021,36(02):46-57.

[7]蓝寿荣.消法视角下的电子商务平台安全保障义务[J].政法论丛,2023(02):37-46.

[8]刘召成.违反安全保障义务侵权责任的体系构造[J].国家检察官学院学报,2019,27(06):53-66.

[9]钟晓雯.数据交易的权利规制路径:窠臼、转向与展开[J].科技与法律(中英文),2021,(05):34-44.

[10]王瑆.数据交易场所的机制构建与法律保障——以数据要素市场化配置为中心[J].江汉论坛,2021(09):129-137.

[11]史宇航.数据交易法律问题研究[D].上海交通大学,2020：162.

[12]莫杨燊.大数据时代公共图书馆读者个人信息安全保障义务探究[J].图书馆理论与实践,2023(05):87-95.

[13]王泽鉴.侵权行为[M].北京:北京大学出版社,2009：175-176.

[14]陆青.电子商务平台经营者安全保障义务的规范构造[J].浙江社会科学,2021(11):70-79+158.

[15]魏昀天.电子商务平台安全保障义务的实证考察与理论进路[J].法律适用,2021(03):34-44.